View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Elsevier - Publisher Connecto

MATHEMATICS Proceedings A 84 (3), September 28, 1981

# On the diophantine equation $(2y^2-3)^2=x^2(3x^2-2)$ in connection with the existence of non-trivial tight 4-designs

by R.J. Stroeker

*Econometric Institute, Erasmus University, P.O. Box 1738, 3000 DR Rotterdam, the Netherlands*

Communicated by Prof. J.H. van Lint at the meeting of October 25, 1980

## 1. INTRODUCTION

The object of this paper is to fill the final gap in the proof of Noboru Ito's theorem [7] on the existence of non-trivial tight 4-designs. To this end, we prove the following theorem:

THEOREM. The Diophantine equation

$$(2y^2-3)^2=x^2(3x^2-2) \tag{1.1}$$

has precisely two solutions in non-negative rational integers $x$ and $y$, namely $x=y=1$ and $x=y=3$.

We follow the notation of [7]. Let $v, k, t$ and $\lambda$ be positive rational integers, subject to $v>k\geqq t$. A $t$-design on $v$ points with block size $k$ and index $\lambda$ or, for short a $t-(v,k,\lambda)$ design, is a pair $(X, \mathscr{A})$, where $X$ is a finite set of points and $\mathscr{A}$ a family of subsets of $X$ (the blocks) such that:

(i) $|X|=v$
(ii) $|A|=k$ for all $A\in\mathscr{A}$
(iii) for each $t$-subset $T$ of $X$, there are exactly $\lambda$ blocks $A$ containing $T$.

If $\mathscr{A}$ consists of all the $k$-subsets of $X$, then $(X, \mathscr{A})$ is called trivial. Moreover, a $t$-design is tight if, roughly speaking, the number of blocks is minimal. In case $t=4$, this minimal number is $\frac{1}{2}v(v-1)$.

Tight 2-designs are the symmetric designs and many examples are known. On

the other hand, tight $2s$-designs with $s \geqq 2$ are apparently extremely rare; cf. [1]. For more information on design theory, the reader is advised to consult [4].

Now Ito's theorem ([7], p. 493) asserts that the only non-trivial tight 4-designs are the well-known 4-(23, 7, 1) and 4-(23, 16, 52). However, in the proof given, a host of errors occurred, some of which seemed irrepairable (cf. [8]). In the recent paper [5] the gap in the proof of Ito's theorem is filled up to at most a finite number of tight 4-designs resulting from the integer solutions of equation (1.1) (cf. [5], p. 42 (24)).

Our theorem shows that the only tight 4-designs resulting from the solutions of (1.1) are trivial.

We return to equation (1.1). In the next section we shall reduce the problem of solving (1.1) to an equivalent but easier to handle problem. More precisely, in section 2 we show the relation between solutions of (1.1) and units of a certain type in a given quartic number field $K$. This number field is investigated in section 3, a particular sequence of algebraic integers of $K$ is considered in section 4 and the last section is devoted to the completion of the proof of the theorem.

## 2. REDUCTION OF THE PROBLEM

In this section our main goal is to prove

LEMMA 1. If $(x, y)$ is a non-negative solution of (1.1), then non-negative integers $U$ and $V$ exist such that

$$U^4 - 24UV^3 + 24V^4 = 1 \tag{2.1}$$

and $x = U^2 - 2UV + 4V^2$, $\pm y = U^2 + 2UV - 6V^2$.

PROOF. Let $(x, y)$ be a solution of (1.1) with $x \geqq 1$ and $y \geqq 1$. If $y = 1$, then $x^2(3x^2 - 2) = 1$ and hence $x = 1$. This solution corresponds with the values $U = 1$, $V = 0$ in (2.1). Hence, if necessary, we may assume that $y \geqq 2$. It is a direct consequence of (1.1) that an integer $z$ exists such that

$$3x^2 - 2 = z^2 \text{ and } 2y^2 - 3 = xz \ (x, y, z \geqq 1).$$

It follows easily that both $x$ and $z$ are odd and that $1 \leqq x \leqq z$. Now put $u := \frac{1}{2}(z + x)$ and $v := \frac{1}{2}(z - x)$. Then $u, v \geqq 0$ and

$$u^2 - 4uv + v^2 = 1, u^2 - v^2 + 3 = 2y^2. \tag{2.2}$$

Hence $u^2 - v^2 + 3(u^2 - 4uv + v^2) = 2y^2$ and thus

$$2u^2 - 6uv + v^2 = y^2. \tag{2.3}$$

It is readily seen from (2.2) that $u$ is even and $v$ is odd. Consequently also $y$ is odd. Write (2.3) as

$$\{\tfrac{1}{2}(v - 3u - y)\}\{\tfrac{1}{2}(v - 3u + y)\} = 7(\tfrac{1}{2}u)^2. \tag{2.4}$$

We assert that the factors of the left-hand side in (2.4) are relatively prime.

Indeed, if $p$ were a prime divisor of both $\frac{1}{2}(v-3u-y)$ and $\frac{1}{2}(v-3u+y)$, then $v-3u\equiv 0 \pmod p$, $y\equiv 0 \pmod p$ and $7(\frac{1}{2}u)^2\equiv 0 \pmod{p^2}$ would lead to $p$ dividing both $u$ and $v$, which contradicts (2.2).

Now suppose $v-3u-y>0$. Then $v-3u+y>0$ and hence $2u<3u<v$ or $0<v-3u<v-2u$. From (2.3) we deduce that $(v-3u)^2=7u^2+y^2>7u^2$ and this yields $v-3u>u\sqrt{7}$. Moreover, (2.2) implies $(v-2u)^2=1+3u^2<4u^2$ and consequently $v-2u<2u$. All this leads to the contradiction:

$$v-2u<2u<u\sqrt{7}<v-3u<v-2u.$$

So $v-3u-y<0$ and $v-3u+y<0$ (note that $u=0$ gives $y=1$).

From (2.4) it follows that

$$\tfrac{1}{2}(v-3u-y)=-a^2 \text{ (resp. } -7b^2) \text{ and } \tfrac{1}{2}(v-3u+y)=-7b^2 \text{ (resp. } -a^2)$$

for certain relatively prime positive integers $a$ and $b$.

This gives $v-3u=-a^2-7b^2$ and $u=2ab$. So

(2.5) $\quad u=2ab, v=-a^2+6ab-7b^2$ with $hcf(a,b)=1$.

Inserting these expressions for $u$ and $v$ into (2.2): $u^2-4uv+v^2=1$, yields after some calculation

$$a^4-4a^3b+6a^2b^2-28ab^3+49b^4=1$$

or

(2.6) $\quad (a-b)^4-24(a-b)b^3+24b^4=1.$

On putting $U:=a-b, V:=b$ equation (2.6) reduces to (2.1).

Moreover, $x=u-v=a^2-4ab+7b^2=U^2-2UV+4V^2$ and $\pm y=a^2-7b^2=U^2+2UV-6V^2$. □

The implication of lemma 1 is clear: equation (2.1) is a norm equation. That is to say, (2.1) may be written as

(2.7) $\quad \mathrm{Norm}_{\mathbb{Q}(\theta)/\mathbb{Q}}(U-V\theta)=1,$

where $\theta$ is a root of $t^4-24t+24=0$. Thus, solving (1.1) means finding all units in $\mathbb{Q}(\theta)$ of the form $U-V\theta$.

## 3. A QUARTIC NUMBER FIELD

The biquadratic polynomial $f(t):=t^4-24t+24$ has discriminant $D(f)=-2^{12}3^37^2$. Hence, $f$ has two real zeros and one pair of complex conjugate ones. One of those real zeros is $\theta:=\sqrt{3}+\sqrt{2\sqrt{3}-3}$. Define $K:=\mathbb{Q}(\theta)$. Dirichlet's unit theorem then tells us that the group of units in $\mathcal{O}_K$ – the ring of integers in $K$ – is the direct product of the cyclic group of order 2 ($+1$ and $-1$ are the only roots of unity) and a free abelian group of rank 2.

We are interested in the following properties of the number field $K$.

LEMMA 2. If $\theta:=\sqrt{3}+\sqrt{2\sqrt{3}-3}$ and $\xi:=-1+\frac{1}{2}(1+\sqrt{3})\theta$ then the number field $K:=\mathbb{Q}(\theta)$ has the following properties:

(1) The number $\xi$ is an algebraic integer and $K=\mathbb{Q}(\xi)$.
(2) A basis for the ring of integers $\mathcal{O}_K$ is given by $\{1,\xi,\xi^2,\xi^3\}$.
(3) The integers $\xi$ and $2+\sqrt{3}=\xi^{-1}(1+\xi+\xi^2)$ form a pair of fundamental units of $\mathcal{O}_K$.
(4) The quadratic number field $\mathbb{Q}(\sqrt{3})$ is a subfield of $K$ and $\mathbb{Q}(\sqrt{3})$ is precisely the set of all elements of $K$ which are left fixed by the conjugation map $K\to K'=K, \xi\mapsto\xi'=\xi^{-1}$.

PROOF. (1) It is easily verified that $\xi$ is a real root of $g(t)$ where $g(t):=t^4-2t^3-2t+1$. Further, $\theta=1-\xi+3\xi^2-\xi^3$ and $28\xi=-4+8\theta+6\theta^2+\theta^3$ and thus $\mathbb{Q}(\theta)=\mathbb{Q}(\xi)$.

(2) The discriminant of $g$ has the value $D(g)=-2^6 3^3$. Consequently, the absolute discriminant of $K$ is negative and a divisor of $2^6 3^3$. It is no more than a routine matter to check that $\{1,\xi,\xi^2,\xi^3\}$ is indeed an integral basis (see: [6], § 29 Satz 1, p. 122).

(3) We note that also $K=\mathbb{Q}(\zeta)$, where $\zeta:=(12)^{\frac{1}{4}}$. Indeed, $\xi=\frac{1}{4}(2+2\zeta+\zeta^2)$ and $\zeta=-2+\xi-2\xi^2+\xi^3$. But then Berwick ([2], p. 372, (22)) gives $\xi, 2+\sqrt{3}$ as a fundamental pair of units.

(4) Since $\sqrt{3}=\xi^{-1}(1-\xi+\xi^2)$, $\mathbb{Q}(\sqrt{3})$ is a subfield of $K$. Both $\xi$ and $\xi^{-1}$ are zeros of $g(t)=t^4-2t^3-2t+1$ and thus $\xi^{-1}$ is a field conjugate of $\xi$. Now $\alpha:=a+b\xi+c\xi^2+d\xi^3=a+b\xi^{-1}+c\xi^{-2}+d\xi^{-3}$ if and only if $0=b(\xi-\xi^{-1})+c(\xi^2-\xi^{-2})+d(\xi^3-\xi^{-3})=(\xi-\xi^{-1})(b+c+3d+(c+2d)\sqrt{3})$ if and only if $b+d=c+2d=0$ if and only if $\alpha=a+d(2-\xi-\xi^{-1})\in\mathbb{Q}(\sqrt{3})$. □

As a consequence of this lemma, we may write (2.7) as

$$U-V\theta=\sigma\xi^a(2+\sqrt{3})^b \text{ with } \sigma=\pm 1 \text{ and } a,b\in\mathbb{Z}. \tag{3.1}$$

As before $\theta=\sqrt{3}+\sqrt{2\sqrt{3}-3}=(\sqrt{3}-1)(\xi+1)=1+\xi^2(2+\sqrt{3})^{-1}$ and hence (3.1) becomes

$$(2+\sqrt{3})(U-V)-V\xi^2=\sigma\xi^a(2+\sqrt{3})^{b+1} \tag{3.2}$$

with $\sigma=\pm 1$ and $a,b\in\mathbb{Z}$. Combining (3.2) with its conjugate equation ($\xi\mapsto\xi^{-1}$):

$$(2+\sqrt{3})(U-V)-V\xi^{-2}=\sigma\xi^{-a}(2+\sqrt{3})^{b+1} \tag{3.3}$$

yields

$$-\sigma V=(2+\sqrt{3})^{b+1}\xi^{2-a}\cdot\frac{\xi^{2a}-1}{\xi^4-1} \tag{3.4}$$

and

$$-\sigma(U-V)=(2+\sqrt{3})^b\xi^{4-a}\cdot\frac{\xi^{2a-4}-1}{\xi^4-1}. \tag{3.5}$$

In particular, it follows from (3.4) that $(\xi^{2a}-1)/(\xi^4-1)\in\mathcal{O}_K$. Consequently, $a\equiv 0 \pmod 2$. Put $a=:2k, k\in\mathbb{Z}$ and define for all $n\in\mathbb{Z}$

$$S_n:=\xi^{2-2n}\cdot\frac{\xi^{4n}-1}{\xi^4-1}.$$

Then equations (3.4) and (3.5) may be written as, respectively,

$$-\sigma V=(2+\sqrt{3})^{b+1}S_k \tag{3.6}$$

and

$$-\sigma(U-V)=(2+\sqrt{3})^{b}S_{k-1}. \tag{3.7}$$

In the next section we shall investigate the sequence $(S_n)_n$.

## 4. A RELATED SEQUENCE

Let $\xi$ be defined as in lemma 2 and, as before,

$$S_n=\xi^{2-2n}.\frac{\xi^{4n}-1}{\xi^4-1}$$

for all $n\in\mathbb{Z}$. The relevant information on the sequence $(S_n)_n$ is given in the following lemma.

LEMMA 3.

(1) $S_{-n}=-S_n$ for all $n\in\mathbb{Z}$.
(2) $S_n\in\mathbb{Z}[\sqrt{3}]$ for all $n\in\mathbb{Z}$.
(3) $S_{n+1}=S_kS_{n-k+2}-S_{k-1}S_{n-k+1}$ for all $k,n\in\mathbb{Z}$.
(4) If $\mathfrak{P}=(1+\sqrt{3})$ the unique prime ideal divisor of 2 in the ring $\mathbb{Z}[\sqrt{3}]$, then
  (i) $S_n$ is divisible by $\mathfrak{P}$ iff $n\equiv 0 \pmod 2$,
  (ii) If $n=\pm 2^{\lambda}m$ with $\lambda\geqq 1$ and $m$ odd, then $\mathfrak{P}^{2\lambda+1}$ exactly divides $S_n$.

PROOF. (1) is trivial and (3) just a routine check. Assertion (2) follows from lemma 2 (4), because $S_n$ is obviously an algebraic integer. To prove (4), we observe that $S_0=0, S_1=1$ and $S_2=2(1+\sqrt{3})$. Moreover, it follows from (3) that $S_{n+1}=2(1+\sqrt{3})S_n-S_{n-1}$ and this implies that $\mathfrak{P}$ does not divide $S_m$ for odd $m$. Furthermore, $S_{2k}=S_k(S_{k+1}-S_{k-1})$ and hence, if $n=2^{\lambda}m$ with $\lambda\geqq 1$ and $m$ odd, we have

$$S_n=S_m\prod_{i=1}^{\lambda}(S_{2^{i-1}m+1}-S_{2^{i-1}m-1}). \tag{4.1}$$

Observe that $S_{k+1}-S_{k-1}=2(1+\sqrt{3})S_k-2S_{k-1}$. This means that, using (i), we may deduce:

$\mathfrak{P}^2$ exactly divides $S_{k+1}-S_{k-1}$ in case $k\equiv 0 \pmod 2$ and
$\mathfrak{P}^3$ exactly divides $S_{k+1}-S_{k-1}$ in case $k\equiv 1 \pmod 2$.

Hence, by means of (4.1), we see that $\mathfrak{P}^3(\mathfrak{P}^2)^{\lambda-1}=\mathfrak{P}^{2\lambda+1}$ exactly divides $S_n$. This completes the proof of the lemma. □

## 5. PROOF OF THE THEOREM

If $(x,y)$ is a non-negative solution of (1.1), then there are non-negative integers $U$ and $V$ such that $U^4-24UV^3+24V^4=1$ or $\mathrm{Norm}_{K/\mathbb{Q}}(U-V\theta)=1$ and

thus $U-V\theta=\sigma\xi^a(2+\sqrt{3})^b$ with $\sigma=\pm 1$ and $a,b\in\mathbb{Z}$, from which we deduced

$$-\sigma V=(2+\sqrt{3})^{b+1}S_k,\ -\sigma(U-V)=(2+\sqrt{3})^bS_{k-1}$$
with $\sigma=\pm 1$ and $b,k\in\mathbb{Z}$.

All this has been shown in the previous sections via equations (2.1), (2.7), (3.1), (3.6) and (3.7).

Now suppose that $S_k\neq 0$ and also $S_{k-1}\neq 0$. Then either $k$ is even and there is a positive rational integer $\lambda$ such that $\mathfrak{P}^{2\lambda+1}$ exactly divides $S_k$, or $k-1$ is even and $\mathfrak{P}^{2\lambda+1}$ exactly divides $S_{k-1}$ for some positive rational integer $\lambda$ (see lemma 3). So either $V$ or $U-V$ is exactly divisible by $\mathfrak{P}^{2\lambda+1}$ for some positive rational integer $\lambda$. This is clearly impossible, for both $V$ and $U-V$ are rational integers and consequently (if even) exactly divisible by an even power of $\mathfrak{P}$. Hence either $S_k=0$ or $S_{k-1}=0$. This can only happen for $k=0, k=1$ respectively. So the only possibilities for $U$ and $V$ are: $V=0, U-V=\pm 1$ and $U-V=0, V=\pm 1$. These possible values for $U$ and $V$ correspond with the two solutions $(x,y)=(1,1)$ and $(3,3)$ as is easily deduced from lemma 1.

This completes the proof of the theorem. □

## 6. POSTSCRIPT

After completing this paper, it was brought to the authors attention that A. Bremner independently obtained the same result following ideas of Cassels and Skolem; cf. [3].

The author wishes to thank the referee for his valuable suggestions.

## REFERENCES

1. Bannai, E. – On tight designs. Quart. J. Math. Oxford (2), **28**, 433-448 (1977).
2. Berwick, W.E.H. – Algebraic number fields with two independent units. Proc. London Math. Soc. **34**, 360-378 (1932).
3. Brenner, A. – A Diophantine equation arising from tight 4-designs. Osaka J. Math. **16**, 353-356 (1979).
4. Cameron, P.J. and J.H. van Lint – Graph theory, Coding theory and Block designs. London Math. Soc. Lect. Note Ser. 19, Cambridge Un. Press (1975).
5. Enomoto, H., N. Ito and R. Noda – Tight 4-designs. Osaka J. Math. **16**, 39-43 (1979).
6. Holzer, L. – Zahlentheorie, Teil I. B.G. Teubner, Leipzig (1958).
7. Ito, N. – On tight 4-designs. Osaka J. Math. **12**, 493-522 (1975).
8. Ito, N. – Corrections and supplements to "On tight 4-designs". Osaka J. Math. **15**, 693-697 (1978).
9. London, H. and R. Finkelstein – On Mordell's equation $y^2-k=x^3$. Bowling Green State Un. Press (1973).
10. Mordell, L.J. – Diophantine equations. Academic Press, London and New York (1969).
11. Noda, R. – On orthogonal arrays of strength 4 achieving Rao's bound. J. London Math. Soc. (2), **19**, 385-390 (1979).
12. Stroeker, R.J. – On the Diophantine equation $x^3-Dy^2=1$. Nieuw Arch. Wisk. (3), **XXIV**, 231-254 (1976).
13. Stroeker, R.J. – On a Diophantine equation of E. Bombieri. Proc. Kon. Ned. Akad. Wetensch. (= Indag. Math.) Serie A, **80**, (2) 131-139 (1977).